What is claimed is

1. A cryptography method, comprising:

determining information to be encrypted; and

encrypting said information using an arithmetic which is not associative.

2. A method as in claim 1, wherein said encrypting comprises using a non-trivial ci-quasigroup to encode.

3. A method as in claim 2, further comprising decoding using the crossed-inverse function of said ci-quasigroup.

4. A method as in claims 1 or 2, wherein said encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using said first result, and encryption can be iterated an arbitrary number of times.

5. A method as in claim 2 further comprising defining a rule indicative of said quasigroup.

6. A method as in claim 3 further comprising defining a rule indicative of said crossed inverse of said quasigroup.

7. A method as in claim 1 further comprising carrying

out a second encrypting using said arithmetic, and wherein a result of said second arithmetic is encrypted exponentially more than a result of said first arithmetic.

8. A method as in claim 1 wherein said encrypting comprises using a non trivial a non-group crossed inverse quasigroup to encode.

9. A method as in claim 3 further comprising distributing information indicative of said quasigroup as a public key, and keeping secret the crossed inverse quasigroup.

10. A method as in claim 2 wherein said quasigroup is formed by an n by n square, where n is greater than 10^{10}.

11. A method as in claim 4 wherein said first and second encryption form iterative encipherment.

12. A method as in claim 4 wherein said first interiation is carried out in a different direction than said first encryption.

13. A method as in claim 12 wherein said first direction is left to right and said second direction is right to left.

14. A method as in claim 1 wherein said encrypting is carried out using block ciphers.

15. A method as in claim 14 wherein said block cipher are defined by a function.

16.A method as in claim 14 wherein said block ciphers are formed using cross inversed quasigroups, used according to $C = f(M,K)$ for the encryption and $M=f_{inv}(C,K)$ for the decryption.

17. A method as in claim 1 wherein said encrypting uses XIP neofields.

18. A method as in claim 1 wherein said encrypting uses near rings.

19. A cryptography method, comprising:

determining information to be encrypted; and

encrypting said information using an arithmetic which is not commutative.

20. A method as in claim 19, wherein said encrypting comprises using a quasigroup to encode.

21. A method as in claim 19, further comprising decoding using a crossed inverse of said quasigroup.

22. A method as in claim 1, wherein said encrypting comprises carrying out a first encryption to get a first

result, then carrying out a second encryption using said first result.

23. A cryptography method comprising encrypting information using an arithmetic with an algebraic structure, said algebraic structure being a nongroup, nonfield structure.

24. A method as in claim 23 wherein said algebraic structure is not associative.

25. A method as claim 23 wherein said algebraic structure is not commutative.

26. A method as in claim 24 wherein said algebraic structure is not commutative.

27. A method as in claim 23 wherein said arithmetic is a crossed inverse quasigroup.

28. A method as in claim 24 wherein said method uses a near ring.

29. An apparatus comprising a program stored on a computer readable media including instructions to:

encrypt a message using a non-associative arithmetic; and

send the encrypted message.

30. An apparatus as in claim 29, wherein said arithmetic includes a non-trivial crossed inverse quasigroup.

31. An apparatus as in claim 29, wherein said arithmetic is one which is based on a multiplication table which is expressed as a rule.

32. An apparatus as in claim 29, further comprising adding a random seed to said arithmetic.

33. An apparatus as in claim 30, further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption.

34. A method of encrypting in a computer, comprising:

obtaining, in the computer, a file to be encrypted;

using a non-associative arithmetic to encrypt the file; and

using another non-associative arithmetic to further encrypt the once-encrypted file.